UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 11754 East Stockton Street, Adelanto, CA 92301	)	Case No. 2:18-MJ-02959

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 21, United States Code, Section 846	See attached Affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

Andrew Truong, DEA Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

_____
Judge's signature

City and state: Los Angeles, California

United States Magistrate Judge
Printed name and title

AUSAs: Lindsey Dotson (x4443), Joseph Axelrad (x7964)

ATTACHMENT A-3

PREMISES TO BE SEARCHED

The premises located at 11754 East Stockton Street, Adelanto, CA 92301 ("SUBJECT PREMISES 3"). SUBJECT PREMISES 3 is a single-story residence located on the north side of East Stockton Street. It has a tile roof, two-car garage, and white concrete driveway leading to the garage from the street. The front door is on the left side of the garage, and there are windows on each side of the front door. SUBJECT PREMISES 3 includes any and all vehicles, storage facilities, outbuildings, and garages within the curtilage of the premises.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are the fruits, instrumentalities, and evidence of violations of 21 U.S.C. § 846 (Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances); 21 U.S.C. §§ 841(a)(1) (Distribution and Possession with Intent to Distribute Controlled Substances); 18 U.S.C. § 924(c) (Carrying or Using a Firearm in Furtherance of a Drug Trafficking Crime or Crime of Violence); 18 U.S.C. § 241 (Conspiracy Against Rights); 18 U.S.C. § 242 (Deprivation of Rights Under Color of Law); 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 666 (Federal Program Bribery); 18 U.S.C. § 1346 (Honest Services Fraud); 18 U.S.C. § 1956 (Money Laundering); and 18 U.S.C. § 1957 (Money Laundering in Property from Specified Unlawful Activity) (collectively, the "Subject Offenses"):

a. Any controlled substance, including but not limited to marijuana;

b. Any items or paraphernalia used for manufacturing, distributing, packaging, and/or weighing controlled substances, including, but not limited to: plastic baggies, scales, and other weighing devices;

c. Any items used in the packaging of currency for consolidation and transportation, including, but not limited to: money-counting machines, money wrappers, rubber bands, duct tape or wrapping tape, plastic wrap, and plastic sealing machines;

d. Any records, documents, programs, applications, or materials showing payment, receipt, concealment, transfer, or movement of money generated from the sale or distribution of marijuana or other controlled substances or from bribery payments, including but not limited to: bank account records, wire transfer records, bank statements, pay-owe sheets, receipts, safe deposit box keys and records, money containers, financial records, and notes, including documents written in vague or coded language;

e. Any drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

f. Jackets or other clothing with the word “sheriff” or other law enforcement identifiers;

g. Law enforcement duty belt and related equipment, including but not limited to: handcuffs, batons, flashlight, gloves, and radio;

h. Records or documents purporting to be, or relating to, search warrants;

i. One black safe that is approximately five feet tall and two feet deep and has a digital combination keypad, white lettering above the keypad, one chrome handle with approximately three spokes, and hinges on the right side of the safe when facing the front of the safe;

j. One black safe that is approximately five feet tall and four feet deep and has one chrome handle with approximately five spokes;

k. Any United States currency over $1,000 or bearer instruments worth over $1,000 (including cashier's checks and traveler's checks);

l. Any records, documents, programs, applications, or materials reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other valuable items;

m. Any records, documents, programs, applications, or materials reflecting the names, addresses, telephone numbers, or communications of members or associates involved in drug trafficking activities or a bribery scheme, including but not limited to: personal telephone books, address books, telephone bills, photographs, videotapes, facsimiles, personal notes, receipts, and documents;

n. Any weapons, including but not limited to: knives, firearms (including pistols, handguns, shotguns, rifles, assault weapons, and machine guns), magazines used to hold ammunition, silencers, and components of firearms (including components or tools which can be used to modify firearms or ammunition);

o. Any indicia of occupancy, residency, or ownership of the SUBJECT VEHICLE, PREMISES, and DEVICES and things described in the warrant, including, but not limited to: forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust

deeds, lease or rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

p. Any documents or records referencing the rental of trucks or other vehicles used to commit the Subject Offenses; and

q. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

r. With respect to any digital device used to facilitate the above-listed Subject Offenses or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. Evidence of the attachment of other devices;

iv. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. Evidence of the times the device was used;

vi. Passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. Records of or information about Internet Protocol addresses used by the device; and

ix. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony

PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of

the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, with respect to a person who is in possession of a SUBJECT DEVICE or any adult person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, the law enforcement personnel are authorized to: (1) depress the thumb and/or fingerprints of the person onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of the person with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Table of Contents

AFFIDAVIT

I, ANDREW TRUONG, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Drug Enforcement Administration ("DEA") and have been so employed since April 2015. I am currently assigned to the DEA's Los Angeles Field Division, High Intensity Drug Trafficking Area Group 48 ("HIDTA 48"), investigating large-scale drug trafficking organizations operating in the Southern California area and elsewhere.

2. I received 640 hours of narcotics law enforcement training at the DEA Basic Agent Training at the DEA Academy, Quantico, Virginia. Through the DEA Academy and continuing education, I have received extensive training on conducting federal narcotics investigations, investigative techniques, running undercover operations, interviewing witnesses and subjects, developing sources, and search and seizure of evidence, among other things.

3. Based on my training, experience, and conversations with other narcotics investigators, I am familiar with drug traffickers' methods of operation including the distribution, storage, and transportation of drugs, as well as the collection of drug proceeds and methods of money laundering used to conceal the nature of the proceeds. I have received training and collaborated with other law enforcement officers regarding the unlawful importation, possession, and distribution of controlled

substances. Based on my experience and work with other law enforcement agents, I am familiar with public corruption statutes and money laundering statutes involving the proceeds of specified unlawful activities and conspiracies associated with criminal narcotics, in violation of Titles 18 and 21 of the United States Code. I also speak regularly with narcotics investigators at the federal, state, and local level, as well as drug traffickers and informants, regarding the manner in which drug traffickers store, sell, and transport narcotics.

4. Prior to joining DEA, I was an Investigative Specialist with the Federal Bureau of Investigation ("FBI") in Los Angeles, California from September 2012 to April 2015. During my tenure with the FBI, I conducted surveillance operations and provided investigative support.

II. PURPOSE OF AFFIDAVIT

5. This affidavit is made in support of a criminal complaint against, and arrest warrants for, ANTRIM MARC ANTRIM ("ANTRIM") and ERIC RODRIGUEZ, also known as "Rooster"[1] ("RODRIGUEZ"), for Conspiracy to Distribute Controlled Substances, in violation of 21 U.S.C. § 846. This affidavit is also made in support of search warrants for the SUBJECT VEHICLE, PREMISES, and DEVICES, as detailed herein and described in Attachments A-1 through A-8, for the items to be seized as

[1] Based on my involvement in this investigation and conversations with other law enforcement officers familiar with RODRIGUEZ, I am aware that he is also known as "Rooster."

described in Attachment B. Attachments A-1 through A-8 and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my training and experience, review of recordings, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrants, and search warrants. It does not purport to set forth all of my knowledge of, or investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. PROPERTY TO BE SEARCHED

7. This affidavit is made in support of a search warrant for the following SUBJECT VEHICLE, PREMISES, and DEVICES:

a. SUBJECT VEHICLE 1. A white 2016 Dodge RAM truck with vehicle identification number 3C63RPGL2GG139703 and California license plate number 89372K2, as described in Attachment A-1, for the items to be seized described in Attachment B;

b. SUBJECT PREMISES 2. The premises located at 1062 East Gladstone Street, Glendora, CA 91740 ("SUBJECT PREMISES 2"), as described in Attachment A-2, for the items to be seized described in Attachment B;

c. SUBJECT PREMISES 3. The premises located at 11754 East Stockton Street, Adelanto, CA 92301 ("SUBJECT

PREMISES 3"), as described in Attachment A-3, for the items to be seized described in Attachment B;

d. SUBJECT PREMISES 4. The premises located at 11042 Andrews Street, South El Monte, CA 91733 ("SUBJECT PREMISES 4"), as described in Attachment A-4, for the items to be seized described in Attachment B;

e. SUBJECT PREMISES 5. An equipment bag locker bearing number "118" located at the Los Angeles County Sheriff's Department ("LASD") Temple Station, as described in Attachment A-5, for the items to be seized described in Attachment B;

f. SUBJECT PREMISES 6. A locker bearing number "130" located in the men's locker room at the LASD Temple Station, as described in Attachment A-6, for the items to be seized described in Attachment B;

g. SUBJECT DEVICE 7. Any digital device, including but not limited to a cellular telephone, in the possession, custody, or control of ANTRIM at the time of his arrest, as described in Attachment A-7, for the items to be seized described in Attachment B; and

h. SUBJECT DEVICE 8. Any digital device, including but not limited to a cellular telephone, in the possession, custody, or control of RODRIGUEZ at the time of his arrest, as described in Attachment A-8, for the items to be seized described in Attachment B.

IV. ITEMS TO BE SEIZED

8. The items to be seized are the evidence, fruits, and instrumentalities of violations of the following: 21 U.S.C.

§ 846 (Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances); 21 U.S.C. §§ 841(a)(1) (Distribution and Possession with Intent to Distribute Controlled Substances); 18 U.S.C. § 924(c) (Carrying or Using a Firearm in Furtherance of a Drug Trafficking Crime or Crime of Violence); 18 U.S.C. § 241 (Conspiracy Against Rights); 18 U.S.C. § 242 (Deprivation of Rights Under Color of Law); 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 666 (Federal Program Bribery); 18 U.S.C. § 1346 (Honest Services Fraud); 18 U.S.C. § 1956 (Money Laundering); and 18 U.S.C. § 1957 (Money Laundering in Property from Specified Unlawful Activity) (collectively, the "Subject Offenses"), as described in Attachment B.

V. SUMMARY OF PROBABLE CAUSE

9. Early in the morning on or about October 29, 2018, ANTRIM, an off-duty LASD deputy sheriff, RODRIGUEZ, and others known and unknown were involved the robbery of an indoor marijuana distribution warehouse, located on Commercial Street in Los Angeles, California. ANTRIM, RODRIGUEZ, and their co-conspirators stole approximately 600 pounds of marijuana and two safes containing about $100,000 in cash.

10. At the time of the robbery, ANTRIM and at least two of his co-conspirators were armed and falsely portrayed themselves to be LASD deputies executing a search warrant or conducting other official business at the warehouse. During the robbery, which lasted approximately two hours, ANTRIM detained three employees working at the warehouse (two security guards and

another employee) in the backseat of an official LASD Ford Explorer. When Los Angeles Police Department ("LAPD") officers responded to a call for service at the warehouse, ANTRIM falsely represented that he was conducting a legitimate search, thereby prompting the LAPD officers to leave the scene and allowing ANTRIM, RODRIGUEZ, and his co-conspirators time to complete the robbery.

VI. PROBABLE CAUSE

A. Background

11. Based on my conversations with LASD Sergeant Investigator Vincent Choi ("Sergeant Choi") and involvement in this investigation, I am aware that ANTRIM is an LASD deputy sheriff.[2] At the time of the robbery detailed herein, ANTRIM was not on duty. He works as a patrol deputy at Temple Station in Temple City, California. He is not currently assigned to a narcotics unit, is not a detective, and would have no reason to investigate or execute a search warrant of the marijuana distribution warehouse, which is located in the City of Los Angeles outside the areas served by the Temple City Station.[3]

12. According to Sergeant Choi, there is no record of RODRIGUEZ being employed as an LASD deputy sheriff.

[2] Sergeant Choi is a member of LASD's Internal Criminal Investigations Bureau, a section of the LASD charged with investigating crimes committed by LASD employees.

[3] According to www.temple.lasd.org (last visited November 4, 2018), the LASD Temple City Stations serves the Chantry Flats, Monrovia-Arcadia-Duarte area, City of Bradbury, City of Duarte, City of Rosemead, City of South El Monte, Temple City, North San Gabriel-East Pasadena area, and South San Gabriel. The marijuana distribution warehouse is in the jurisdiction patrolled by LAPD.

B. Surveillance Video Captures ANTRIM, RODRIGUEZ, and Co-conspirators Robbing the Marijuana Distribution Warehouse While Armed and Purporting to be Deputies

13. Based on my conversations with Sergeant Choi, I am aware that an attorney at the law firm representing the owner of the marijuana distribution warehouse contacted Sergeant Choi on or about November 2, 2018. According to Sergeant Choi, the attorney stated the following:

a. In the early morning hours of October 29, 2018, approximately 600 pounds of marijuana (packaged for bulk distribution) and two safes containing approximately $100,000 in United States currency were stolen from the warehouse by individuals purporting to be LASD deputies.

b. An employee of the warehouse, who was present during the robbery, reported that one of the vehicles involved in the robbery had a California license plate bearing number 1488363.

c. According to Sergeant Choi, a black Ford Explorer bearing California license plate number 1488363 is an LASD-registered vehicle assigned to the LASD Temple Station. ANTRIM, through his work at the LASD Temple Station, would have had access to this vehicle.

14. Sergeant Choi also told me that the aforementioned attorney gave him security camera footage from the warehouse on two USB thumb drives. The footage was captured from approximately 32 cameras located throughout the warehouse and purports to show events at the warehouse from approximately 3:00 a.m. to 5:00 a.m. on or about October 29, 2018.

15. I reviewed the security camera footage and observed the following:

a. At approximately 3:09 a.m.[4], a black unmarked Ford Explorer (the "Ford Explorer") drove by the warehouse.[5] At approximately 3:11 a.m., the Ford Explorer appeared on the driveway to the warehouse behind a closed gate. ANTRIM was the driver.[6] ANTRIM exited the car, got the attention of an individual believed to be a male security guard for the warehouse, and showed the guard a piece of paper inside a folder.[7] The security guard then opened the gate, and ANTRIM drove the Ford Explorer into the parking lot of the warehouse.

b. After ANTRIM drove the Ford Explorer into the parking lot, he and two other men exited the car. ANTRIM appeared to be wearing a duty belt[8] with a holstered firearm. (In later footage, it also appears that the two co-conspirators

---

[4] The times are based on the timestamps I observed in the security footage.

[5] I conducted surveillance at the address provided to be by Sergeant Choi and observed a commercial-looking warehouse resembling what I observed in the surveillance video. It appeared to be a functioning business with multiple employees on the premises.

[6] Sergeant Choi told me that he has met ANTRIM in person. Sergeant Choi stated that he reviewed the footage and recognized the driver as ANTRIM. In addition, I have a reviewed an LASD personnel photograph of ANTRIM and also recognize ANTRIM as the driver of the Ford Explorer.

[7] Based on my training and experience and involvement in this investigation, it is possible that ANTRIM showed the guard a document purporting to be a search warrant for the warehouse in order to gain entry to the premises.

[8] A duty belt is a type of belt often worn by law enforcement officers that usually contains handcuffs, a radio, and a firearm, among other things.

who arrived with ANTRIM were wearing duty belts, each with holstered firearms.) One of the co-conspirators who arrived with ANTRIM also appeared to be holding a long gun[9], possibly an assault rifle or shotgun. ANTRIM was wearing a green vest that said "sheriff." The other two were wearing green jackets with what appeared to be LASD patches on the sleeve.

c. ANTRIM then placed that security guard and another individual, who also appeared to be a male security guard, in the backseat of the Ford Explorer.

d. At approximately 3:15 a.m., ANTRIM approached the front door of the warehouse and displayed what appeared to be an LASD deputy sheriff badge to an unknown female employee sitting behind the front desk of the reception area. ANTRIM showed her a piece of paper in a folder. She then allowed ANTRIM and the two co-conspirators to enter the warehouse. She lifted her shirt to show her waist, as if to indicate to ANTRIM that she was unarmed. ANTRIM then returned to the Ford Explorer and drove it closer to the front door. He then placed the unknown female employee in the backseat of the Ford Explorer with the two male security guards.[10]

e. At approximately 3:21 a.m., a white Penske moving truck (the "Penske Truck") arrived at the warehouse and parked

[9] A long gun is a type of firearm with a longer barrel than other classes of firearms.

[10] DEA has not yet conducted interviews of these three witnesses or other employees who work at the warehouse. The existence of the investigation is not yet known to the public or targets, and openly conducting interviews at this time may comprise the integrity of the investigation and lead to the destruction of evidence or flight of subjects or targets.

by the front door. The driver of the Penske Truck appeared to be a third male co-conspirator. He was in plain clothes and not wearing an LASD jacket.

f. While at the warehouse, ANTRIM and his three co-conspirators removed multiple boxes, dark-colored garbage bags, and large clear bags of what appeared to be marijuana from the warehouse and placed the items into the Penske Truck.

g. At approximately 3:43 a.m., several marked LAPD police cars began arriving at the warehouse.[11] As the LAPD police cars arrived, ANTRIM walked toward the front gate of the warehouse's parking lot. At the same time, the three co-conspirators fled the warehouse through a back roll-up door. Two of them discarded their LASD jackets. One appeared to throw his LASD jacket and other items in a bush next to the warehouse. Another placed his LASD jacket on top of a portable basketball hoop stand near the back roll-up door before leaving.

h. At approximately 3:50 a.m., ANTRIM appeared to meet with multiple LAPD officers who had arrived on scene. At approximately 3:53 a.m., ANTRIM re-entered the warehouse. He retrieved the discarded LASD jacket left on the portable basketball hoop stand, along with a duty belt that too had been left behind. He took those items to the warehouse parking lot and put them in the trunk of the Ford Explorer.

[11] Sergeant Choi informed me that he reviewed LAPD calls for service on or about October 29, 2018 and learned that a caller reported that individuals purporting to be officers were attempting to execute a search warrant at the warehouse.

i. At approximately 3:57 a.m., ANTRIM met with multiple LAPD officers once again in the front parking lot of the warehouse. At approximately 4:00 a.m., ANTRIM appeared to be on a cellular telephone as the group of LAPD officers stood near him. At approximately 4:12 a.m., an LAPD officer appeared to be talking on the cellular telephone, which he then handed to ANTRIM at approximately 4:14 a.m. Shortly thereafter, the LAPD officers left the warehouse parking lot. Around that time, ANTRIM appeared to make at least one phone call.[12]

j. At approximately 4:16 a.m., ANTRIM continued to load additional boxes containing clear plastic bags of what appeared to be marijuana into the back of the Penske Truck.

k. At approximately 4:34 a.m., after the LAPD officers had left, a white Dodge RAM Dually pick-up truck (the "Dodge RAM Dually") arrived at the warehouse parking lot. RODRIGUEZ was the driver.[13] Another man, possibly one of the

[12] Sergeant Choi informed me that some of the responding LAPD officers were interviewed regarding their interaction with ANTRIM. One of them said that ANTRIM handed him a cellular telephone that was in the middle of a call. The screen of the phone displayed a particular individual's name, who is in fact another LASD deputy. According to the LAPD officer, the person on the phone claimed that he was ANTRIM's sergeant and that ANTRIM was working in an official capacity. According to Sergeant Choi, the individual with whom the LAPD officer purportedly spoke was not ANTRIM's sergeant. Based on my training and experience and involvement in this investigation, I believe that the person on ANTRIM's phone falsely told the LAPD officer that he was ANTRIM's sergeant and that DEFEDANT was at the warehouse on official business.

[13] I have spoken with other law enforcement investigators who are familiar with RODRIGUEZ and have seen him in person. Those investigators have reviewed screen shots of the video footage from the warehouse robbery and identified the driver of the Dodge RAM Dually as RODRIGUEZ.

individuals previously at the warehouse with ANTRIM, got out of the Dodge RAM Dually. He and RODRIGUEZ then went inside the warehouse. Based on my training and experience and involvement in this investigation, I believe that the Dodge RAM Dually RODRIGUEZ drove to the warehouse is the same Dodge RAM that is registered to him (SUBJECT VEHICLE 1).[14]

l. At approximately 4:35 a.m., an unidentified co-conspirator, possibly one of the individuals previously at the warehouse with ANTRIM, approached the rear of the warehouse. He appeared to retrieve the LASD jacket and other items that had been previously discarded into the bushes. He then left the warehouse and returned shortly thereafter.

m. At approximately 4:50 a.m., ANTRIM, RODRIGUEZ, and two co-conspirators moved two large safes from the warehouse to the Penske Truck.

i. One black safe was approximately five feet tall and two feet deep and had a digital combination keypad, white lettering above the keypad, one chrome handle with approximately three spokes, and hinges on the right side of the safe when facing the front of the safe.

[14] According to law enforcement database queries, a 2016 Dodge RAM with vehicle identification number 3C63RPGL2GG139703 and California license plate number 89372K2 is registered to RODRIGUEZ. From the video, I observed that the license plate for the Dodge RAM Dually contained the numbers "9372" and therefore was consistent with the license plate for SUBJECT VEHICLE 1. Based on my experience, I know that a Dodge RAM Dually is a type of Dodge RAM. A Dually has four wheels in the back of the truck, as opposed to a standard vehicle with two wheels in the back.

ii. The other black safe was approximately five feet tall and four feet deep and had one chrome handle with approximately five spokes.

n. At approximately 4:56 a.m., RODRIGUEZ and two co-conspirators left the warehouse in the Penske Truck and Dodge RAM Dually. ANTRIM then released the three warehouse employees from the back of the Ford Explorer and left.

C. ANTRIM Was Not Executing a Lawful Search Warrant

16. Based on my training and experience, review of the security camera footage described above, and conversations with other law enforcement officers, I do not believe that ANTRIM was acting in his official capacity to conduct a lawful search of the warehouse for the following reasons, among others:

a. As noted, ANTRIM was not on duty. He works as a patrol deputy at Temple Station in Temple City, California. He is not currently assigned to a narcotics unit, is not a detective, and would have no reason to investigate or execute a search warrant of the warehouse, which is located in the City of Los Angeles outside the areas served by the Temple City Station.

b. Sergeant Choi indicated to me that he has no evidence from his review of LASD records and conversations with others at LASD that there was any legitimate search warrant executed at the warehouse on or about October 29, 2018. Based on my training and experience, the execution of a legitimate search warrant often requires extensive coordination with other on-duty law enforcement partners and would be known to others at LASD in order to dispatch appropriate resources and personnel to

assist with the search and seizure, and to ensure officer safety. In addition, prior to executing a search, an operational plan with details regarding the anticipated search and seizure is usually submitted to a supervisor for review and approval. Sergeant Choi is unaware of ANTRIM submitting any operational plan.

c. Finally, and most telling, when LAPD officers responded to the warehouse, ANTRIM's three co-conspirators fled. Two of them discarded their LASD jackets. They only returned to the warehouse after LAPD officers had left. Based on my training and experience, law enforcement officers conducting a search are not trained to leave the premises of a lawful search in this manner and do not shed their clothing or other paraphernalia identifying as them as law enforcement. In fact, legitimate law enforcement officers often wear clothing indicating that they are law enforcement for their own safety. Visual identifiers indicating who is law enforcement are important during a search so that an officer, particularly one carrying a firearm, is not advertently mistaken for a criminal. The fact that ANTRIM's co-conspirators fled and shed their LASD jackets shows consciousness of guilt that they knew they were not legitimate law enforcement conducting a legal search and seizure.

D. The SUBJECT VEHICLE, PREMISES, and DEVICES

17. SUBJECT VEHICLE 1. SUBJECT VEHICLE 1 is a white 2016 Dodge RAM truck with vehicle identification number 3C63RPGL2GG139703 and California license plate number 89372K2,

as described in Attachment A-1. For the following reasons, among others, I believe that SUBJECT VEHICLE 1 is RODRIGUEZ's truck and is the same Dodge RAM Dually that RODRIGUEZ drove to the warehouse during the robbery:

a. From my review of the surveillance camera footage of the warehouse robbery, I observed RODRIGUEZ drive a white Dodge RAM Dually matching the description of SUBJECT VEHICLE 1 into the warehouse parking lot during the robbery. Although I could not ascertain the entire license plate of the Dodge RAM Dually, I saw that it had the numbers "9372" in the middle of the license plate. The license plate of the Dodge RAM Dually was therefore consistent with the license plate number for SUBJECT VEHICLE 1. According to law enforcement queries, SUBJECT VEHICLE 1 has California license plate number 89372K2 and is registered to RODRIGUEZ.[15]

b. A law enforcement agent conducting an open source search of Facebook told me that she observed a photograph of RODRIGUEZ standing in front of a white truck matching the description of SUBJECT VEHICLE 1.

18. SUBJECT PREMISES 2. SUBJECT PREMISES 2 is the premises located at 1062 East Gladstone Street, Glendora, CA 91740 ("SUBJECT PREMISES 2"), as described in Attachment A-2. Based on my conversations with other law enforcement agents, I

[15] In addition to RODRIGUEZ, SUBJECT VEHICLE 1 is jointly registered to another individual at an address in Compton, California. Based on my involvement in this investigation and conversations with other investigators, I believe that the address in Compton may be the home of a relative or associate of RODRIGUEZ.

know that there was a tracking device on the Penske Truck that recorded the location of the truck during and following the robbery. This data was maintained by the rental company in the regular course of business and not activated at the request of the government. A review of that data shows that the Penske Truck went to SUBJECT PREMISES 2 on or about October 29, 2018 after the robbery. On or about November 5, 2018, agents surveilling ANTRIM observed individuals loading one large object covered by a tarp into the back of a truck at SUBJECT PREMISES 2. The object looked similar in size and shape to one of the safes stolen during the warehouse robbery. Agents observed ANTRIM, as well as SUBJECT VEHICLE 1 (RODRIGUEZ's Dodge RAM truck), at or near SUBJECT PREMISES 2 around the time this object was being moved. Agents also observed ANTRIM removing boxes from SUBJECT PREMISES 2 and loading them into another vehicle.[16]

19. SUBJECT PREMISES 3. SUBJECT PREMISES 3 is the premises located at 11754 East Stockton Street, Adelanto, CA 92301, as described in Attachment A-3. I believe that RODRIGUEZ resides at SUBJECT PREMISES 3 for the following reasons, among others:

a. According to law enforcement queries, RODRIGUEZ is the property owner of SUBJECT PREMISES 3. He also has at least one vehicle registered to him at SUBJECT PREMISES 3.

[16] Although some evidence may have been removed from this location, based on my training and experience, I believe that evidence of the Subject Offenses is still likely to be found at this location.

Based on my training and experience, individuals often register vehicles to their home address or an address they frequent.

b. Recent surveillance has shown RODRIGUEZ and SUBJECT VEHICLE 1 (which belongs to RODRIGUEZ) at SUBJECT PREMISES 3. A DEA task force officer informed me that he saw SUBJECT VEHICLE 1 parked on the driveway of SUBJECT PREMISES 3 at approximately 9:00 a.m. on or about November 5, 2018. He also saw RODRIGUEZ on the street immediately west of the driveway for SUBJECT PREMISES 3 the same day at approximately 9:10 a.m. At approximately 11:45 p.m. on or about November 5, 2018, a law enforcement officer observed SUBJECT VEHICLE 1 parked on the driveway of SUBJECT PREMISES 3. A law enforcement officer also observed RODRIGUEZ seated at a table inside the garage of SUBJECT PREMISES 3 (the garage door was open) the following day, on or about November 6, 2018 at approximately 1:00 p.m.

c. GPS data for a phone believed to be used by RODRIGUEZ also suggests that RODRIGUEZ resides at SUBJECT PREMISES 3. On or about November 6, 2018 at approximately 12:40 a.m., DEA began receiving the data pursuant to a warrant.[17] According to law enforcement agents who have reviewed the data and are familiar with this case, GPS data indicated that the phone believed to be used by RODRIGUEZ was at or near SUBJECT

[17] On November 5, 2018, the Honorable Alka Sagar, United States Magistrate Judge, signed a warrant in case no. 18-MJ-2956 authorizing (1) the disclosure of historical cell-site information and prospective cell site and GPS information and (2) use of a cell-site simulator for two phones, including one believed to be used by RODRIGUEZ.

PREMISES 3 during the early morning hours of November 6, 2018. The data is consistent with RODRIGUEZ spending the night at SUBJECT PREMISES 3.

20. SUBJECT PREMISES 4. SUBJECT PREMISES 4 is the premises located at 11042 Andrews Street, South El Monte, CA 91733, as described in Attachment A-4. Based on physical surveillance and an analysis of GPS and cell-site data from ANTRIM's phone, I believe that ANTRIM is currently residing at SUBJECT PREMISES 4 for the following reasons, among others[18]:

a. GPS data obtained pursuant to a warrant on ANTRIM's phone suggests that ANTRIM spent the night at SUBJECT PREMISES 4 on November 5, 2018.[19] The GPS data, which I have reviewed, indicates that ANTRIM's phone was at or near SUBJECT PREMISES 4 throughout the night on November 5, 2018 and into the morning on November 6, 2018. Moreover, from conversations with other law enforcement personnel, I am aware that surveilling officers observed ANTRIM leave SUBJECT PREMISES 4 through a side gate by the garage in the morning on November 6, 2018. The combination of the GPS data from ANTRIM's phone and agent surveillance leads me to believe that ANTRIM spent the night on November 5, 2018 at SUBJECT PREMISES 4.

---

[18] Although a review of public records does not list ANTRIM as the owner of SUBJECT PREMISES 4, I am aware from my experience that individuals may rent, as opposed to own, their homes or may cohabitate with the owner of the property.

[19] On November 5, 2018, the Honorable Maria Audero, United States Magistrate Judge, signed a warrant in case no. 18-MJ-2946 authorizing (1) the disclosure of historical cell-site information and prospective cell site and GPS information and (2) use of a cell-site simulator for ANTRIM's phone.

b. Furthermore, the historical cell-site data obtained pursuant to the warrant on ANTRIM's phone suggests that ANTRIM has been living at SUBJECT PREMISES 4 for at least a month. (Prior to that, cell-site data and other records suggest that he was living elsewhere.) An FBI special agent and trained member of the FBI's Cellular Analysis Survey Team ("CAST") conducted a preliminary analysis of the historical cell-site data for ANTRIM's phone. According to the agent, for the month of October and continuing through the present, ANTRIM's phone has connected to the cellular tower within approximately 400 meters of SUBJECT PREMISES 4 more often than to any other tower. Moreover, based upon the agent's review of "beginning and ending usage,"[20] it appears that ANTRIM is accessing the phone in the vicinity of SUBJECT PREMISES 4 when he goes to sleep and then again when he wakes up. In light of this information, combined with the law enforcement surveillance showing ANTRIM at SUBJECT PREMISES 4 and my training and experience, I believe that ANTRIM is currently residing at SUBJECT PREMISES 4.

21. SUBJECT PREMISES 5. SUBJECT PREMISES 5 is an equipment bag locker bearing number "118" located at the LASD Temple Station, as described in Attachment A-5. According to Sergeant Choi, SUBJECT PREMISES 5 is an equipment bag locker assigned to ANTRIM. Sergeant Choi told me that deputies usually

[20] When someone goes to sleep, they often will not send text messages or make phone calls for an extended period of time. This extended period of inactivity for text messages and phone calls can be indicative of when an individual is sleeping.

keep paperwork and equipment, such as a helmet or baton, in these lockers.

22. SUBJECT PREMISES 6. SUBJECT PREMISES 6 is a locker bearing number "130" located in the men's locker room at the LASD Temple Station, as described in Attachment A-6. According to Sergeant Choi, SUBJECT PREMISES 6 is a locker assigned to ANTRIM. Sergeant Choi told me that deputies usually keep articles of clothing, vests, handcuffs, duty belts, and other similar items in these lockers.

23. SUBJECT DEVICE 7. SUBJECT DEVICE 7 is any digital device, including but not limited to a cellular telephone, in the possession, custody, or control of ANTRIM at the time of his arrest, as described in Attachment A-7.

24. SUBJECT DEVICE 8. SUBJECT DEVICE 8 is any digital device, including but not limited to a cellular telephone, in the possession, custody, or control of RODRIGUEZ at the time of his arrest, as described in Attachment A-8.

VII. TRAINING AND EXPERIENCE REGARDING THE SUBJECT OFFENSES

A. Training and Experience Regarding Drug Trafficking

25. Based on my training and experience and conversations with agents and other law enforcement officers trained and experienced in narcotics investigations, I am familiar with the methods and modes of operation typically used by individuals trafficking in controlled substances. Based on conversations with other law enforcement officers and my knowledge of this investigation and others, I am aware of the following:

a. Individuals involved in the illegal distribution of controlled substances, or who possess controlled substances with the intent to distribute to controlled substances, will frequently keep records, documents, United States currency derived from their criminal conduct, and other evidence pertinent to their drug trafficking activities at their residence and areas associated with their residence. They often conceal evidence of their drug trafficking in their residences, as well as garages, carports, storage facilities, lockers, outbuildings, and other surrounding areas to which they have ready access. Further, I know from my conversations with Assistant United States Attorney Lindsey Greer Dotson ("AUSA Dotson") that the case law in the Ninth Circuit establishes a general presumption that individuals involved in drug trafficking maintain evidence of their criminal activities in their residences.[21]

b. Drug traffickers, including individuals who assist drug traffickers, will often conceal controlled substances, proceeds of their illegal activity, and weapons in

[21] AUSA Dotson provided me the following case citations: "In the case of drug dealers, evidence is likely to be found where the dealers live." United States v. Angulo-Lopez, 791 F.2d 1394, 1399 (9th Cir. 1986) (citations omitted). "[E]vidence discovered by [] officers linking the ANTRIMs to a drug scheme provide[s] 'more than a sufficient showing for obtaining the warrant to search [their]...residence.'" United States v. Fannin, 817 F.2d 1379, 1382 (9th Cir. 1987) (quotation and citation omitted). An unpublished decision refers to this common-sense principle as the "residency presumption." United States. v. Crowell, 1993 WL 493743, *2 (9th Cir. 1993) (unpublished).

hidden compartments or manufactured spaces, including within the walls of their residences and garages, within furniture contained in their residences, and in compartments in their vehicles.

c. The distribution of drugs is generally a continuing criminal activity taking place indefinitely unless interrupted by law enforcement action. Drug traffickers typically will obtain and distribute controlled substances on a regular basis, much as any distributor of a legitimate commodity would purchase stock for sale. Such traffickers will have an "inventory" which will fluctuate in size depending on the demand for the product.

d. Drug traffickers begin distributing small quantities of controlled substances. As they develop their customer base and their supply contacts, they are able to deal in larger quantities. Those who are trafficking in distribution quantities of controlled substances, i.e. quantities significantly beyond those which are used for personal or recreational use (as is the case here), are not new to the business; rather, they have usually established their supply contacts and customers over months or years and are likely to have records of their past business, contacts, and customers in their residence.

e. Drug traffickers, including individuals who assist drug traffickers, often have in their possession, including at their residence, firearms -- including handguns, pistols, revolvers, rifles, shotguns, machine guns, and/or other

weapons, as well as ammunition and ammunition components -- that are used to protect and secure the drug traffickers' property. In addition, as was the case here, firearms are often used to facilitate the theft of controlled substances and cash. Some of the firearms and other protective gear used by the robbers in this case may be issued by a law enforcement agency and thus may be stored in official lockers or containers.

f. Drug traffickers, including individuals who assist drug traffickers, often have in their possession large amounts of cash from their criminal endeavors. Drug traffickers generally sell controlled substances for cash. Because drug traffickers generally sell controlled substances for cash, they typically have significant amounts of cash on hand, as proceeds of sales and to purchase their own supplies. In addition, drug traffickers and those who assist drug traffickers often have other assets generated by their criminal conduct or purchased with cash earned, such as precious metals and stones, jewelry, real estate, vehicles, and other valuables. They often keep these items, and records reflecting their purchase or sale, such as automobile titles or deeds to property, as well as evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money acquired from engaging in drug trafficking activities, in their residences, offices, garages, storage buildings, lockers, automobiles, and safe deposit boxes.

g. Drug traffickers, including individuals who assist drug traffickers, often attempt to conceal the proceeds

of their criminal activity through money laundering transactions to make it appear as though the proceeds were derived from a legitimate source.

h. Drug traffickers, including individuals who assist drug traffickers, often communicate with co-conspirators using coded or vague language to thwart the detection of law enforcement. Therefore, documents, notes, communications, or other records evidencing criminal conduct may be in coded or vague language.

i. Drug traffickers, including individuals who assist drug traffickers, often use one or more telephones, pagers, or other digital devices to negotiate times, places, schemes, and manners for importing, possessing, concealing, manufacturing, and distributing controlled substances, and for arranging transport and security of the same as well as for the disposition of proceeds from the sale of controlled substances. For instance, in this case, I know that ANTRIM used a cellular phone to contact an individual who purported to be ANTRIM's sergeant and who falsely told an LAPD officer that ANTRIM was at the warehouse on official business. In addition, it is possible that ANTRIM used his cellular phone to inform his co-conspirators who had fled the warehouse that the LAPD officers had left and that it was safe to return.

j. Furthermore, I know that professional drug trafficking operations depend upon maintaining both long-distance and local contacts with both suppliers and those down the organizational chain to the local traffickers. They often

use fraudulent information to subscribe to communication facilities, especially cellular telephones, maintain separate customer and supplier telephones, and frequently change communications facilities to thwart law enforcement efforts to intercept their communications. They frequently use pre-paid telephones and/or false or misleading subscriber information as a way of distancing themselves from criminal liability.

k. Data contained on digital devices used by drug traffickers and their co-conspirators often includes, among other things, records of telephone calls, text messages, and e-mail communications between the trafficker and the co-conspirators; Global Positioning System ("GPS") information and other location information that can help identify stash locations, meeting places, and trafficking routes; and identifying information about the trafficker and co-conspirators, such as contact lists, calendar appointments, and photographs or videos.

l. Drug traffickers, including individuals who assist drug traffickers, often maintain in their residences documents relating to their communication devices, in the form of receipts, bills, telephone and address books, and other books and papers that reflect, among other things, the names, addresses, and/or telephone numbers of their customers, co-conspirators, and associates in the drug trafficking organization.

m. Drug traffickers commonly provide controlled substances to trusted distributors in their organization on

credit and commonly obtain controlled substances from their suppliers on credit. Therefore, I am aware that drug traffickers maintain books, records, customer lists, receipts, notes, ledgers, and other papers relating to the transportation, receipt, ordering, sales, and distribution of narcotics, narcotics proceeds, and equipment, and that such documents may be in code to attempt to thwart law enforcement detection.

n. Drug traffickers, including individuals who assist drug traffickers, keep records of their illegal activities for a period of time extending beyond the time during which they actually possesses particular controlled substances, in order to maintain contact with criminal associates for future transactions, and to have records of prior transactions for which they might still be owed payment or might owe someone else money.

o. Drug traffickers, including individuals who assist drug traffickers, generally continue their criminal activity for extensive periods of time, ordinarily indefinitely. Indeed, individuals who have established an income based on drug sales or distribution tend to continue the activity for prolonged periods of time because that is how they make or supplement their living and maintain the lifestyle to which they have become accustomed.

B. Training and Experience Regarding Public Corruption

26. ANTRIM is a deputy sheriff -- and therefore a public official -- who has used his status as a law enforcement officer to undermine and thwart the detection of legitimate law

enforcement. Based on my training and experience investigating narcotics crimes, knowledge of this investigation and others, and my conversations with law enforcement officers trained to investigate public corruption crimes, I am familiar with the methods and modes of operation utilized by corrupt law enforcement officers engaged in drug trafficking and other crimes. In particular, based on my training and experience, knowledge of this investigation and others, and conversations with other law enforcement officers, I am aware of the following:

a. Because many public officials do not gain tremendous wealth from their government paycheck alone, it is important for those involved in criminal activities to conceal unexplained wealth and unexplained cash, often including from their family and friends. It is common practice for individuals engaged in public corruption and fraud crimes to store and hide United States currency and financial instruments fraudulently or inappropriately obtained in their residences, home offices, garages, and safe deposit boxes. They often possess safes, locked containers, and/or hidden containers at their residence in order to store and conceal proceeds of the crime. In addition, they often have safe deposit boxes and off-site storage facilities to store and hide proceeds of their crimes and possess the keys and other related documents to those boxes and storage facilities at their residence.

b. It is also common practice for individuals engaged in public corruption and fraud crimes to store other

evidence of their criminal conduct -- such as records of past bribe payments or contact information for individuals involved in the corrupt scheme -- at their residences.

c. Individuals involved in public corruption or fraud crimes often attempt to conceal the proceeds of their criminal activity through money laundering transactions to make it appear as though the proceeds were derived from a legitimate source.

d. Individuals engaged in public corruption and fraud crimes often have other assets generated by their criminal conduct, or purchased with cash earned in order to conceal large cash proceeds, such as precious metals and stones, jewelry, real estate, vehicles, and other valuables. These individuals often keep these items, and records reflecting their purchase or sale, such as automobile titles or deeds to property, as well as evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money acquired from engaging in their criminal activities, in their residences, home offices, garages, lockers, automobiles, and safe deposit boxes. They do this in order to keep track of the value of the items and the cash they have received from their illicit activities.

e. Individuals engaged in public corruption and fraud crimes often use one or more telephones, pagers, or other digital devices to discuss the corrupt scheme and payments. Data contained on digital devices used by individuals engaged in public corruption and fraud crimes often include, among other

things, records of telephone calls, text messages, and e-mail communications between the target and other co-conspirators; Global Positioning System ("GPS") information and other location information that can help identify meeting places; and identifying information about the target and other co-conspirators paying bribes, such as contact lists, calendar appointments, and photographs or videos.

f. Individuals engaged in public corruption and fraud crimes often maintain in their residences documents relating to their communication devices, in the form of receipts, bills, telephone and address books, and other books and papers that reflect, among other things, the names, addresses, and/or telephone numbers of their co-conspirators in the corrupt scheme.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

27. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy

disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory

or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an

active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image

as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone

else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

28. As discussed herein, based on my training and experience, I believe that digital devices will be found during the search. For instance, based on my review of the surveillance video, I observed ANTRIM using a cellular phone during the robbery in an effort, it appeared, to communicate with co-conspirators. The cellular phone I observed ANTRIM using appeared to be a smartphone, which is a multi-purpose mobile computing device. Based on my experience, smartphones are a more advanced type of cellular phone that usually have a biometric unlock feature.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five

Instrumentality Protocol

fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with

characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To

activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

29. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

30. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can

Instrumentality Protocol

occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

31. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also

possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the SUBJECT PREMISES and reasonably believed by law enforcement to be a user of the device to unlock the device using biometric features in the same manner as discussed in the following paragraph.

32. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every adult person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know

based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

33. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

///

///

IX. CONCLUSION

34. Based on the foregoing, I respectfully submit that there is probable cause to believe that MARC ANTRIM, ERIC RODRIGUEZ, also known as "Rooster," and others known and unknown, engaged in a Conspiracy to Distribute Controlled Substances, in violation of 21 U.S.C. § 846.

35. Furthermore, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses, will be found at or in the SUBJECT VEHICLE, PREMISES, and DEVICES, as described in Attachments A-1 through A-8.

ANDREW TRUONG
Special Agent
Drug Enforcement Administration

Subscribed to and sworn before me this ___ day of November, 2018.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

VEHICLE TO BE SEARCHED

A white 2016 Dodge RAM truck with vehicle identification number 3C63RPGL2GG139703 and California license plate number 89372K2 ("SUBJECT VEHICLE 1").

ATTACHMENT A-2

PREMISES TO BE SEARCHED

The premises located at 1062 East Gladstone Street, Glendora, CA 91740 ("SUBJECT PREMISES 2"). SUBJECT PREMISES 2 is a single-story residence. SUBJECT PREMISES 2 is located on the south side of East Gladstone Street. The residence has a dark-colored roof. The exterior of the residence is white with a blue/gray trim. A concrete walkway leads from the sideway to a red or brown front door. SUBJECT PREMISES 2 has a garage that faces a rear alley. SUBJECT PREMISES 2 includes any and all vehicles, storage facilities, outbuildings, and garages within the curtilage of the premises.

ATTACHMENT A-3

PREMISES TO BE SEARCHED

The premises located at 11754 East Stockton Street, Adelanto, CA 92301 ("SUBJECT PREMISES 3"). SUBJECT PREMISES 3 is a single-story residence located on the north side of East Stockton Street. It has a tile roof, two-car garage, and white concrete driveway leading to the garage from the street. The front door is on the left side of the garage, and there are windows on each side of the front door. SUBJECT PREMISES 3 includes any and all vehicles, storage facilities, outbuildings, and garages within the curtilage of the premises.

ATTACHMENT A-4

PREMISES TO BE SEARCHED

The premises located at 11042 Andrews Street, South El Monte, CA 91733 ("SUBJECT PREMISES 4"). SUBJECT PREMISES 4 is a single-story residence located on the corner of Andrews Street and Lexham Avenue. The residence is brown in color with a brown roof and black metal gate surrounding part of the property. A concrete driveway goes from Andrews Street to a detached two-car garage in the rear. SUBJECT PREMISES 4 includes any and all vehicles, storage facilities, outbuildings, and garages within the curtilage of the premises.

ATTACHMENT A-5

PREMISES TO BE SEARCHED

An equipment bag locker bearing number "118" ("SUBJECT PREMISES 5") located at the Los Angeles Sheriff's Department Temple Station, 8838 Las Tunas Drive, Temple City, CA 91780. SUBJECT PREMISES 5 is beige in color and approximately 2.5 feet wide and 2.5 feet deep. SUBJECT PREMISES 5 has the number "118" on the door.

ATTACHMENT A-6

PREMISES TO BE SEARCHED

A locker bearing number "130" ("SUBJECT PREMISES 6") located inside the men's locker room at the Los Angeles Sheriff's Department Temple Station, 8838 Las Tunas Drive, Temple City, CA 91780. SUBJECT PREMISES 6 is green in color. On the front of SUBJECT PREMISES 6 is the number "130" and a sticker that says "Tacos Omana."

ATTACHMENT A-7

DEVICES TO BE SEARCHED

Any digital device, including but not limited to a cellular telephone, in the possession, custody, or control of MARC ANTRIM, date of birth 10-27-1977, at the time of his arrest.

ATTACHMENT A-8

DEVICES TO BE SEARCHED

Any digital device, including but not limited to a cellular telephone, in the possession, custody, or control of ERIC RODRIGUEZ, also known as "Rooster," date of birth 11-24-1985, at the time of his arrest.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are the fruits, instrumentalities, and evidence of violations of 21 U.S.C. § 846 (Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances); 21 U.S.C. §§ 841(a)(1) (Distribution and Possession with Intent to Distribute Controlled Substances); 18 U.S.C. § 924(c) (Carrying or Using a Firearm in Furtherance of a Drug Trafficking Crime or Crime of Violence); 18 U.S.C. § 241 (Conspiracy Against Rights); 18 U.S.C. § 242 (Deprivation of Rights Under Color of Law); 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 666 (Federal Program Bribery); 18 U.S.C. § 1346 (Honest Services Fraud); 18 U.S.C. § 1956 (Money Laundering); and 18 U.S.C. § 1957 (Money Laundering in Property from Specified Unlawful Activity) (collectively, the "Subject Offenses"):

a. Any controlled substance, including but not limited to marijuana;

b. Any items or paraphernalia used for manufacturing, distributing, packaging, and/or weighing controlled substances, including, but not limited to: plastic baggies, scales, and other weighing devices;

c. Any items used in the packaging of currency for consolidation and transportation, including, but not limited to: money-counting machines, money wrappers, rubber bands, duct tape or wrapping tape, plastic wrap, and plastic sealing machines;

d. Any records, documents, programs, applications, or materials showing payment, receipt, concealment, transfer, or movement of money generated from the sale or distribution of marijuana or other controlled substances or from bribery payments, including but not limited to: bank account records, wire transfer records, bank statements, pay-owe sheets, receipts, safe deposit box keys and records, money containers, financial records, and notes, including documents written in vague or coded language;

e. Any drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

f. Jackets or other clothing with the word “sheriff” or other law enforcement identifiers;

g. Law enforcement duty belt and related equipment, including but not limited to: handcuffs, batons, flashlight, gloves, and radio;

h. Records or documents purporting to be, or relating to, search warrants;

i. One black safe that is approximately five feet tall and two feet deep and has a digital combination keypad, white lettering above the keypad, one chrome handle with approximately three spokes, and hinges on the right side of the safe when facing the front of the safe;

j. One black safe that is approximately five feet tall and four feet deep and has one chrome handle with approximately five spokes;

k. Any United States currency over $1,000 or bearer instruments worth over $1,000 (including cashier's checks and traveler's checks);

l. Any records, documents, programs, applications, or materials reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other valuable items;

m. Any records, documents, programs, applications, or materials reflecting the names, addresses, telephone numbers, or communications of members or associates involved in drug trafficking activities or a bribery scheme, including but not limited to: personal telephone books, address books, telephone bills, photographs, videotapes, facsimiles, personal notes, receipts, and documents;

n. Any weapons, including but not limited to: knives, firearms (including pistols, handguns, shotguns, rifles, assault weapons, and machine guns), magazines used to hold ammunition, silencers, and components of firearms (including components or tools which can be used to modify firearms or ammunition);

o. Any indicia of occupancy, residency, or ownership of the SUBJECT VEHICLE, PREMISES, and DEVICES and things described in the warrant, including, but not limited to: forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust

deeds, lease or rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

p. Any documents or records referencing the rental of trucks or other vehicles used to commit the Subject Offenses; and

q. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

r. With respect to any digital device used to facilitate the above-listed Subject Offenses or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. Evidence of the attachment of other devices;

iv. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. Evidence of the times the device was used;

vi. Passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. Records of or information about Internet Protocol addresses used by the device; and

ix. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony

PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of

the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, with respect to a person who is in possession of a SUBJECT DEVICE or any adult person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, the law enforcement personnel are authorized to: (1) depress the thumb and/or fingerprints of the person onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of the person with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.